(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 274 212 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
08.01.2003 Bulletin 2003/02

(51) Int Cl.[7]: **H04L 29/06**

(21) Application number: **01128220.9**

(22) Date of filing: **28.11.2001**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **04.07.2001 JP 2001202954**

(71) Applicant: **Allied Telesis K. K.**
Shinagawa-ku, Tokyo 141-8635 (JP)

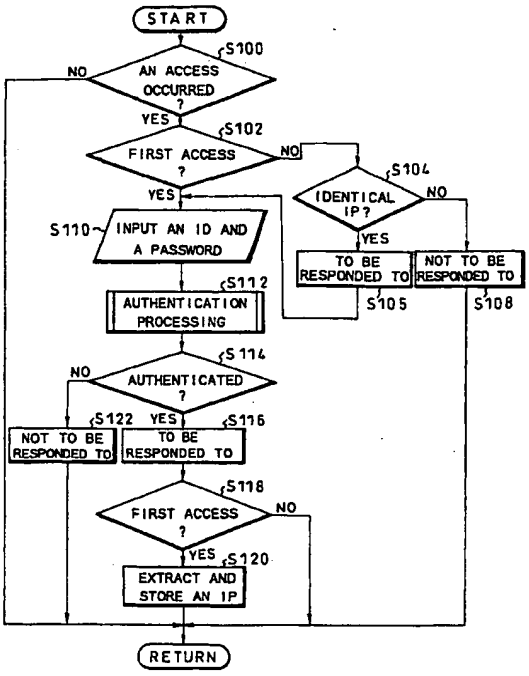
(72) Inventor: **Sato, Takayuki, Allied Telesis K.K**
Tokyo 141-8635 (JP)

(74) Representative: **Gesthuysen, von Rohr & Eggert**
Patentanwälte
Postfach 10 13 54
45013 Essen (DE)

(54) Method and device avoiding unauthorized access

(57) When a first access from an external apparatus occurs to an intelligent interconnecting device and the external apparatus is authenticated in authentication processing based on a TCP/IP protocol in the intelligent interconnecting device, the intelligent interconnecting device stores therein a source IP address of the external apparatus. When an access from an external apparatus occurs thereafter, a response to the access is permitted only when a source IP address of the external apparatus giving the access is identical with the source IP address stored in advance.

FIG. 3



EP 1 274 212 A1

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] The present invention relates to a interconnecting device having a packet repeating function and the like in what is called a LAN (Local Area Network) system, and more particularly to an unauthorized access avoiding method, an unauthorized access avoiding program, a recording medium in which an unauthorized access avoiding program is recorded, an intelligent interconnecting device, and a LAN system which realize security improvement and so on in what is known as an intelligent interconnecting device whose operation is controllable from outside.

[0002] What is known as a packet interconnecting device which is represented by what is called a hub and a router is an apparatus indispensable for configuring a LAN system and various kinds of packet interconnecting devices having various functions in addition to basic functions have been proposed according to forms and so on of LAN systems (for example, refer to Japanese Patent Laid-open No. Hei 5-327720). In some of these interconnecting devices, what is known as management functions such as monitoring operational status and setting operation conditions of the interconnecting devices particularly through communication with external computers are provided and these interconnecting devices are generally called intelligent interconnecting devices.

[0003] In a conventional LAN system to which this intelligent interconnecting device is applied to configure the LAN system, an IP address is given to the intelligent interconnecting device and what is called TCP/IP communication processing is performed for processing communication between a managing computer and the intelligent interconnecting device so that setting, changing, and the like of various operation conditions and so on of the intelligent interconnecting device are controllable by remote control from the managing computer which is connected to the LAN system. More specifically, what is called TCP/IP protocols of various kinds such as TELNET (RFC854), SNMP (RFC1157), TFTP (RFC1350), ICMP (RFC792), and HTTP (RFC1945) are selectively used according to forms of communication between the managing computer and the intelligent interconnecting device.

[0004] For example, unauthorized operation of the intelligent interconnecting device by someone other than a managing party thereof is conventionally prevented in such a manner in which log-in to the intelligent interconnecting device is made possible by the FTP (RFC765), a user identifier and a password are requested to be inputted after the log-in, and only when they are identical with a predetermined identifier and a predetermined password, the access is authenticated as an access from the managing party and the operation thereafter from this outside managing party is permitted.

[0005] However, since security for the intelligent interconnecting device is dependent only on the protocol in the above conventional structure and some of the TCP/IP protocols have no security function, the conventional structure does not always guarantee highly reliable security. In other words, take the above conventional apparatus for example, it does not satisfactorily guarantee security since the authentication by using the inputted user identifier and password after the log-in, which is one of the functions that the FTP has, is not a function which is specially provided from a viewpoint of preventing an unauthorized access to the intelligent interconnecting device and furthermore, it has a disadvantage that an access is easily authenticated as long as the inputted user identifier and password are identical with the predetermined user identifier and password even when the access is from a computer other than the managing computer.

[0006] It is an object of the present invention to provide an unauthorized access avoiding method in an intelligent interconnecting device, an unauthorized access avoiding program for an intelligent interconnecting device, a recording medium in which an unauthorized access avoiding program for an intelligent interconnecting device is recorded, an intelligent interconnecting device, and a LAN system which surely realize prevention of an access from a computer other than a pre-designated computer without depending on a security function of a protocol and/or which improve the security.

[0007] The above object is achieved by a method, device, LAN system, program or recording medium according to any one the independent claims. Preferred embodiments are subject of the subclaims.

[0008] It is a further aspect of the present invention to provide an unauthorized access avoiding method in an intelligent interconnecting device, an unauthorized access avoiding program for an intelligent interconnecting device, a recording medium in which an unauthorized access avoiding program for an intelligent interconnecting device is recorded, an intelligent interconnecting device, and a LAN system which realize strengthening of a security function to improve reliability only with some new functions added to existing software.

[0009] It is still another aspect of the present invention to provide an unauthorized access avoiding method in an intelligent interconnecting device, an unauthorized access avoiding program for an intelligent interconnecting device, a recording medium in which an unauthorized access avoiding program for an intelligent interconnecting device is recorded, an intelligent interconnecting device, and a LAN system which realize simplification of software for guaranteeing security.

[0010] In order to achieve the above objects and aspects of the present invention, according to a first embodiment of the present invention, it is preferably provided an unauthorized access avoiding method in an intelligent interconnecting device having a function of repeating a packet which is transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol, the unauthorized access avoiding method in

an intelligent interconnecting device comprising the following steps:

- when an access from an external apparatus is authenticated through execution of the TCP/IP protocol, extracting and storing a source IP address included in a packet which is transmitted from the external apparatus;
- when an access from an external apparatus occurs thereafter, judging whether or not a source IP address of the external apparatus giving the access is identical with the stored source IP address; and
- only when the source IP address of the external apparatus is judged to be identical with the stored source IP address, permitting communication thereafter between the external apparatus having the source IP address identical with the stored source IP address and the intelligent interconnecting device.

[0011] In this method, after the source IP address of the external apparatus is once authenticated through the execution of the TCP/IP protocol, the source IP address included in the packet which is transmitted from the external apparatus at the time of executing the protocol is extracted and stored so that, when some access occurs from an external apparatus thereafter whose source IP address is judged to be non-identical with the stored source IP address, the external apparatus is determined as an apparatus not to be responded to. Therefore, a conventional disadvantage that an access is permitted even with a non-identical source IP address as long as a user identifier and a password thereof are identical with a predetermined identifier and a predetermined password is surely eliminated. Consequently, security is further improved with a simple structure compared with a conventional method.

[0012] According to a second embodiment of the present invention, an unauthorized access avoiding program which is executed in an intelligent interconnecting device having a function of repeating a packet which is transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol is provided, the unauthorized access avoiding program for an intelligent interconnecting device comprising the following steps:

- a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred;
- a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in the first step that the first access from outside has occurred;
- a third step of causing the intelligent interconnecting device to judge after the authentication processing in the second step whether or not authentication is given;
- a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in the third step that the authentication is given;
- a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from the external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in the fourth step;
- a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in the third step;
- a seventh step of causing the intelligent interconnecting device to judge whether or not the source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in the first step;
- an eighth step of determining the external apparatus whose source IP address is judged to be identical with the stored source IP address as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to process the steps beginning from the second step when the source IP address of the external apparatus is judged to be identical with the stored source IP address in the seventh step; and
- a ninth step of determining the external apparatus whose source IP address is judged to be non-identical with the stored source IP address as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the source IP address of the external apparatus is judged to be non-identical with the stored source IP address in the seventh step.

[0013] This structure is particularly appropriate for carrying out the unauthorized access avoiding method in an intelligent interconnecting device in the first em-

bodiment of the present invention and is realizable, for example, by what is called a microcomputer, or a circuit and software having functions equivalent thereto.

[0014] According to a third embodiment of the present invention, a recording medium in which a computer readable unauthorized access avoiding program which is executed in an intelligent interconnecting device having a function of repeating a packet which is transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol is recorded is provided, wherein the unauthorized access avoiding program comprises the following steps:

- a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred;
- a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in the first step that the first access from outside has occurred;
- a third step of causing the intelligent interconnecting device to judge after the authentication processing in the second step whether or not authentication is given;
- a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in the third step that the authentication is given;
- a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from the external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in the fourth step;
- a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in the third step;
- a seventh step of causing the intelligent interconnecting device to judge whether or not the source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in the first step;
- an eighth step of determining the external apparatus whose source IP address is judged to be identical with the stored source IP address as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to process the steps beginning from the second step when the source IP address of the external apparatus is judged to be identical with the stored source IP address in the seventh step; and
- a ninth step of determining the external apparatus whose source IP address is judged to be non-identical with the stored source IP address as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the source IP address of the external apparatus is judged to be non-identical with the stored source IP address in the seventh step.

[0015] According to a fourth embodiment of the present invention, an intelligent interconnecting device having a function of repeating a packet which is transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol is provided, the intelligent interconnecting device comprising the following:

- a LAN trunk line interfacing section having an interface function with a LAN trunk line;
- a port interfacing section having an interface function with a terminal connected thereto;
- a storage section for storing a program and data therein, and
- a central controlling section for controlling operations of the LAN trunk line interfacing section, the port interfacing section, and the storage section, and wherein the central controlling section processes the following:
- when an access from an external apparatus is authenticated through execution of the TCP/IP protocol, to extract a source IP address included in a packet which is transmitted from the external apparatus and store it in the storage section;
- when an access from an external apparatus occurs thereafter, to judge whether or not a source IP address of the external apparatus giving the access is identical with the stored source IP address; and
- only when the source IP address is judged to be identical with the stored source IP address, to permit communication thereafter with the external apparatus having the source IP address identical with

the stored source IP address.

[0016] Further details, aspects and advantages will be explained with reference to the enclosed drawings. It shows:

FIG. 1 a schematic view showing a structure example of a LAN system according to an embodiment of the present invention;

FIG. 2 a schematic view showing a structure example of an intelligent interconnecting device which is used in the LAN system shown in FIG. 1;

FIG. 3 a subroutine flow chart showing a processing procedure in a first example of unauthorized access avoiding processing executed by the intelligent interconnecting device shown in FIG. 2; and

FIG. 4 a subroutine flow chart showing a processing procedure in a second example of unauthorized access avoiding processing executed by the intelligent interconnecting device shown in FIG. 2.

[0017] Embodiments of the present invention are explained in detail below with reference to the attached drawings.

[0018] It is to be understood that members, arrangements, and so on which are explained below are not restrictive of the present invention and various improvements and modifications may be made within the scope and spirit of the present invention.

[0019] First, the structure of a LAN system to which an intelligent interconnecting device according to an embodiment of the present invention is applied to configure the LAN system is explained with reference to FIG. 1.

[0020] What is called personal computers 2 as a plurality of terminals and a LAN trunk line 3 are connected to an intelligent interconnecting device 1 in this LAN system. To the LAN trunk line 3, at least a managing computer 4 is connected and furthermore, a different network 5 may also be connected. The managing computer 4, which is connected directly to the LAN trunk line 3 in this structure, may alternatively be connected to the LAN trunk line 3 via the different network 5.

[0021] Incidentally, the managing computer 4 may also work as a server or alternatively, the server may be provided separately in addition to the managing computer 4.

[0022] The intelligent interconnecting device 1 is composed of operation and function which are controllable from outside as well as packet interconnecting capability.

[0023] FIG. 2 shows a structure example of the intelligent interconnecting device 1. The structure thereof and so forth are explained below with reference to FIG. 2.

[0024] The intelligent interconnecting device 1 comprises a central controlling section 6, a LAN trunk line interfacing section (shown as 'B-I/F' in FIG. 2) 7, a port interfacing section (shown as 'P-I/F' in FIG. 2) 8, and a storage section 9, which are connected with one another via a common internal bus 10. This structure is not basically different from that of a conventional apparatus except that the central controlling section 6 performs unauthorized access avoiding processing, which is described later.

[0025] The central controlling section 6 performs operation control of the whole intelligent interconnecting device 1 in this structure and particularly, in the embodiment of the present invention, executes the later described unauthorized access avoiding processing.

[0026] The LAN trunk line interfacing section 7 interfaces the intelligent interconnecting device 1 with the LAN trunk line 3 and the port interfacing section 8 interfaces the intelligent interconnecting device 1 with the personal computers 2 as terminals.

[0027] The storage section 9 stores therein various programs to be executed by the central controlling section 6 and also stores data therein which is given thereto and is to be sent out therefrom via the LAN trunk line interfacing section 7 and the port interfacing section 8. The storage section 9 has a storage area whose storage content is not erased even when the power supply is cut off and a storage area whose storage content is erased when the power supply is cut off so that data is selectively stored in the respective areas according to its use and so on. The storage section 9, which is realizable by a generally known storage element and therefore, is not explained in detail, is appropriately structured, for example, by using a hard disk and the like as well as a semiconductor memory such as what is called an RAM and an ROM, and the like.

[0028] Note that, according to the embodiment of the present invention, a TCP/IP protocol is stored in the area of the storage section 9 whose storage content is not erased even when the power supply is cut off, and it is executed by the central controlling section 6 when necessary. Incidentally, among various TCP/IP protocols, any TCP/IP protocol may be used as long as it is appropriate for executing the unauthorized access avoiding processing, which is described later, and more specifically as long as it carries out what is known as authentication processing by using a user identifier and a password.

[0029] Moreover, in the storage section 9, an IP address given in advance to the intelligent interconnecting device 1, and a user identifier (ID) and a password necessary for authentication of an access from an external apparatus based on the TCP/IP protocol are stored in advance in the area whose content is not erased even when the power supply is cut off.

[0030] A first example of the unauthorized access avoiding processing executed by the central controlling section 6 is explained next with reference to FIG. 3.

[0031] To explain first, it is premised that the unauthorized access avoiding processing is executed as one step of subroutine processing in main routine processing executed in the central controlling section 6.

[0032] When the central controlling section 6 starts the processing, it is first judged whether or not an access from outside has occurred to the intelligent interconnecting device 1 (refer to a step S100 in FIG. 3). When it is judged that the access from outside has occurred (YES), the procedure proceeds to a next step S102. Meanwhile, when it is judged in the step S100 that no access from outside has occurred (NO), this subroutine processing is once finished, the procedure returns to the not shown main routine processing, and this subroutine processing is started again after predetermined processing of the main routine processing.

[0033] Then, in the step S102, it is judged whether or not the access to the intelligent interconnecting device 1 from outside is a first access. When the access is judged to be the first access (YES), the procedure proceeds to a next step S110. Meanwhile, when the access is not judged to be the first access (NO), the procedure proceeds to a later described step S104.

[0034] In the step S110, a user identifier (ID) and a password are demanded from an external apparatus giving the access to the intelligent interconnecting device 1 from outside (for example, the managing computer 4) and inputs of the user identifier and the password are received.

[0035] Then, authentication processing for the inputted user identifier and password is performed (refer to a step S112 in FIG. 3).

[0036] Here, the steps S110 and S112 are processed through execution of the generally known TCP/IP protocol. In other words, the TCP/IP protocol, which is premised to be provided in the intelligent interconnecting device 1 according to the embodiment of the present invention, as is explained above in the structure explanation, is appropriately a TCP/IP protocol, in particular, capable of executing the authentication processing by using a user identifier and a password. As such a TCP/IP protocol, for example, TELNET is available. An explanation of a detailed processing procedure of this protocol is omitted here.

[0037] Then, after the authentication processing (refer to the step S112 in FIG. 3) is over, it is judged whether or not the authentication is given (refer to a step S114 in FIG. 3). Here, 'the authentication is given' means that the user identifier and the password are identical with those set in advance in the storage section 9 and the external apparatus giving the access is authenticated. 'The authentication is not given' means that the user identifier and the password are non-identical with those set in advance in the storage section 9 and the external apparatus giving the access is not authenticated.

[0038] When it is judged in the step S114 that the authentication is not given, that is, the external apparatus is not authenticated (NO), a response to the external apparatus is determined to be unallowable (refer to a step S122 in FIG. 3), a series of the subroutine processing is finished, and the procedure returns to the main routine processing for the time being. Then, in the main routine processing, processing for a case in which the response to the external apparatus is determined to be unallowable is performed according to the provided TCP/IP protocol.

[0039] Meanwhile, when it is judged in the step S114 that the authentication is given (YES), the response to the access from the external apparatus is determined to be allowable (refer to a step S116 in FIG. 3) and then, it is judged whether or not the procedure so far is the procedure for the first access from the external apparatus (refer to a step S118 in FIG. 3). Then, when the access from the external apparatus is judged to be the first access (YES), the procedure proceeds to a step S120 described next. Meanwhile, when the access is not judged to be the first access (NO), a series of the subroutine processing is finished and the procedure returns to the main routine processing since processing in the step 120 described next has already been carried out for the access and need not be repeated again.

[0040] In the processing of the step S120, an IP address of a source (the external apparatus) included in a packet which is transmitted from the external apparatus (hereinafter, referred to as a 'source IP address') is extracted and stored in a predetermined area of the storage section 9 (refer to the step S120 in FIG. 3). Note that the storage area for the source IP address in this case is appropriately an area whose storage content is not erased even when the power supply is cut off.

[0041] After the processing of the step S120 is over, a series of the subroutine processing is finished and the procedure returns to the main routine. Then, in the main routine processing, the processing for a case in which the response to the external apparatus is determined to be allowable is carried out according to the provided TCP/IP protocol.

[0042] Meanwhile, when it is judged in the aforesaid step S102 that the access is not the first access and the procedure proceeds to a step S104, it is judged whether or not the source IP address of the external apparatus (for example, the managing computer 4) giving the access is identical with a source IP address stored in the storage section 9 in advance. Incidentally, the source IP address of the external apparatus is recognizable when the source IP address included in a generally known form in the packet which is transmitted to the intelligent interconnecting device 1 from the external apparatus is extracted.

[0043] Then, when it is judged in the step S104 that the source IP address is identical with the stored source IP address (YES), the response to the external apparatus giving the access is determined to be allowable and

the procedure proceeds to the processing of the aforesaid step S110 (refer to the step S106 in FIG. 3). Meanwhile, when it is judged in the step S104 that the source IP address is non-identical with the stored source IP address (NO), the response to the external apparatus is determined to be unallowable, a series of the subroutine processing is finished, and the procedure returns to the main routine (refer to a step S108 in FIG. 3). In the main routine processing, processing for a case in which the response to the external apparatus is determined to be unallowable is performed according to the provided TCP/IP protocol.

[0044] A second example of the unauthorized access avoiding processing which is executed by the central controlling section 6 is explained next with reference to FIG. 4. Note that the same processing as that shown in FIG. 3 is given the same numerals and signs and is not explained in detail. The following explanation focuses mainly on what is different from the processing shown in FIG. 3.

[0045] To summarize the content of the unauthorized access avoiding processing in the second example first, in the structure based on the unauthorized access avoiding processing in the first example shown in FIG. 3, a valid period is set for the source IP address of the external apparatus whose access is to be accepted and moreover, the source IP address which is not identical with the stored one is stored in an unauthorized access IP list and notified to a managing apparatus.

[0046] Specific explanation is given below with reference to FIG. 4. A subroutine processing shown in FIG. 4 is different from the subroutine processing shown in FIG. 3 in that steps S105, S109a, S109b are provided. The other processing content is the same as that in the subroutine processing shown in FIG. 3 and therefore, only processing content in these newly provided steps is explained below.

[0047] First, when the source IP address of the external apparatus (for example, the managing computer 4) giving the access is judged in the step S104 to be identical with the source IP address which is stored in the storage section 9 in advance (YES), it is judged whether or not this source IP address is within the valid period (refer to the step S105 in FIG. 4). In other words, the source IP address of the external apparatus whose access to the intelligent interconnecting device 1 is permitted is stored in the predetermined area of the storage section 9 as described above and the valid period is determined when the source IP address of the external apparatus is first stored. In the step S105, it is judged whether or not the source IP address is within the valid period. Incidentally, time lapse from the time of storing the source IP address needs to be recognized in order to judge whether or not it is within the valid period, which is made possible when what is known as a calendar function or clock function is executed through generally known software processing in the central controlling section 6.

[0048] Then, when the source IP address is judged in the step S105 to be within the valid period (YES), the response to the external apparatus giving the access is determined to be allowable and the procedure proceeds to the processing of the step S110 (refer to the step S106 in FIG. 4).

[0049] Meanwhile, when it is judged in the step S104 that the source IP address is non-identical with the stored source IP address, or is not within the valid period, in other words, the valid period is expired, the response to the external apparatus is determined to be unallowable (refer to the step S108 in FIG. 4) and the source IP address of the external apparatus which is judged to be non-identical with the stored source IP address or not to be within the valid period in the judgment in the step S104 or the step S105 is registered in the unauthorized access IP list (refer to the step S109a in FIG. 4). In short, when an access to the intelligent interconnecting device 1 from outside occurs and a source IP address of the external apparatus giving the access is judged to be non-identical with the stored source IP address in the step S104, the source IP address which is judged to be non-identical is stored in subsequence in the unauthorized access IP list which is provided in a predetermined area of the storage section 9 to register therein the source IP address which is judged to be non-identical with the stored source IP address.

[0050] In order to notify the managing computer 4 of the source IP address which is judged to be non-identical with the stored source IP address, this source IP address is then transmitted as a predetermined packet to the managing computer 4 via the LAN trunk line interfacing section 7 (refer to the step S109b in FIG. 4). After the processing of the step 109b, the procedure returns to the main routine processing and the processing for the case in which the response to the external apparatus is determined to be unallowable is performed according to the provided TCP/IP protocol.

[0051] Incidentally, the source IP address which is judged to be non-identical with the stored source IP address is stored (refer to the step S109a in FIG. 4) and notified to the managing computer 4 (refer to the step S109b in FIG. 4) in the above second example, but only either one of the storage and the notification may be carried out.

[0052] Furthermore, the explanations of both the first and second examples are made on the premise that only one source IP address is stored in the intelligent interconnecting device 1 for the external apparatus whose access is permitted but it is not restrictive that only one source IP address is set and a plurality of them may of course be set.

[0053] When the intelligent interconnecting device 1 is structured to be operable under an SNMP (Simple Network Management Protocol) which is a network control protocol in a TCP/IP network, that is, when the intelligent interconnecting device 1 is provided with an SNMP agent and, for example, the managing computer

4 and other computers are also provided with the SNMP manager, a source IP address of the managing computer 4 is stored in the intelligent interconnecting device 1 as managing apparatus information in order to limit a transmission destination of an event notice (Trap) from the intelligent interconnecting device 1 to a specific computer, for example, only the managing computer 4 so that the Trap is transmitted only to the managing computer 4 and thereby careless spread of information can be prevented.

[0054] Furthermore, the authentication processing in the steps S110, S112 in FIG. 3 and FIG. 4 may be, for example, enciphered to improve security.

[0055] The explanation of the above structure example is made on the premise that the unauthorized access avoiding program for an intelligent interconnecting device to be executed by the central controlling section 6 is stored in a nonvolatile semiconductor memory constituting a part of the storage section 9 which works as a recoding medium of the program and is executed by being read in the central controlling section 6 from the semiconductor memory, but the use of the semiconductor memory is not of course restrictive.

[0056] More specifically, a flexible disk, a CD-ROM, an optical recording medium such as a DVD and a PD, a magneto-optic recording medium such as an MD, a magnetic recording medium, and the like may be used as a recording medium other than the semiconductor memory. Incidentally, special apparatus for reading and writing data are required for some of these recording media and the storage section 9 may of course be constituted by including these apparatus.

[0057] As described above, according to the present invention, the source IP address of the managing computer is extracted and stored from a packet which is received through the execution processing of the existing TCP/IP protocol and communication with an external apparatus having an IP address other than the stored source IP address is not allowed thereafter, which brings about an effect that security, which is not sufficiently secured in a conventional authentication processing by the TCP/IP protocol, is further improved and a system with high reliability can be provided compared with a conventional example.

[0058] Moreover, the authentication processing by the TCP/IP protocol is carried out after the source IP address is judged to be identical with the stored source IP address and therefore, sufficient security is maintained in an intelligent interconnecting device in which TCP/IP protocols of various kinds are provided by executing the authentication processing by one of these protocols. Thereby, the authentication processing by the individual protocols can be omitted. This brings about an effect that software load can be reduced.

[0059] Furthermore, a response to an access by a broadcast can be restricted. This makes it difficult for an outside intruder to recognize the existence of an apparatus to be managed, in other words, the intelligent interconnecting device to be managed by the managing computer, so that security is further improved compared with the conventional example.

[0060] In addition, the user identifier and the password, which are conventionally prepared for each protocol, can be integrated. This brings about an effect that software is allowed to be simplified.

Claims

1. An unauthorized access avoiding method in an intelligent interconnecting device having a function of repeating a packet which is transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol, wherein the method device comprises the steps of:

   extracting and storing a source IP address included in a packet which is transmitted from an external apparatus when an access from the external apparatus is authenticated through execution of the TCP/IP protocol;

   judging, when an access from an external apparatus occurs thereafter, whether or not a source IP address of the external apparatus giving the access is identical with the stored source IP address; and

   permitting communication thereafter between the external apparatus having the source IP address identical with the stored transmitting end IP address and the intelligent interconnecting device only when the source IP address of the external apparatus is judged to be identical with the stored source IP address.

2. Method according to claim 1, **characterized that** the method further comprises the step of registering the source IP address of the external apparatus which is judged to be non-identical in an unauthorized access IP list when the source IP address is judged to be non-identical with the stored source IP address.

3. Method according to claim 1 or 2, **characterized that** the method further comprises the step of notifying an authenticated managing computer of the source IP address of the external apparatus which is judged to be non-identical when the source IP address is judged to be non-identical with the stored source IP address.

4. Method according to any one of the preceding claims, **characterized that** the method further comprises the steps of:

judging whether or not the source IP address which is judged to be identical with the stored source IP address is within a valid period set in advance when the source IP address is judged to be identical with the stored source IP address, and

permitting communication thereafter between the external apparatus having the source IP address which is judged to be within the valid period and the intelligent interconnecting device only when the source IP address of the external apparatus is judged to be within the valid period.

5. An unauthorized access avoiding program which is executed in an intelligent interconnecting device having a function of repeating a packet which is transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol, wherein the program comprises:

a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred;

a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in said first step that the first access from outside has occurred;

a third step of causing the intelligent interconnecting device to judge after the authentication processing in said second step whether or not authentication is given;

a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in said third step that the authentication is given;

a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from the external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in said fourth step;

a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in said third step;

a seventh step of causing the intelligent interconnecting device to judge whether or not the source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in said first step;

an eighth step of determining the external apparatus whose source IP address is judged to be identical with the stored source IP address as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to process the steps beginning from said second step, when the source IP address of the external apparatus is judged to be identical with the stored source IP address in said seventh step; and

a ninth step of determining the external apparatus whose source IP address is judged to be non-identical with the stored source IP address as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the source IP address of the external apparatus is judged to be non-identical with the stored source IP address in said seventh step.

6. An unauthorized access avoiding program which is executed in an intelligent interconnecting device having a function of repeating a packet which is transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol, preferably according to claim 5, wherein the program comprises:

a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred;

a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in said first step that the first access from outside has occurred;

a third step of causing the intelligent interconnecting device to judge after the authentication processing in said second step whether or not

authentication is given;

a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in said third step that the authentication is given;

a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from the external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in said fourth step;

a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in said third step;

a seventh step of causing the intelligent interconnecting device to judge whether or not the source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in said first step;

an eighth step of causing the intelligent interconnecting device to judge whether or not the source IP address is within a predetermined valid period when the source IP address of the external apparatus is judged to be identical with the stored source IP address in said seventh step;

a ninth step of determining the external apparatus having the source IP address which is judged to be within the predetermined valid period as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to execute the steps beginning from said second step, when the source IP address of the external apparatus is judged to be within the predetermined valid period in said eighth step; and

a tenth step of determining the external apparatus whose source IP address is judged to be non-identical or is judged to be not within the predetermined valid period as an apparatus not to be responded to thereafter by the intelligent interconnecting device, when the source IP address of the external apparatus is judged to be non-identical with the stored source IP address in said seventh step or is judged to be not within the predetermined valid period in said eighth step.

7. An unauthorized access avoiding program which is executed in an intelligent interconnecting device having a function of repeating a packet which is transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol, preferably according to claim 5 or 6, wherein the program comprises:

a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred;

a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in said first step that the first access from outside has occurred;

a third step of causing the intelligent interconnecting device to judge after the authentication processing in said second step whether or not authentication is given;

a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in said third step that the authentication is given;

a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from the external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in said fourth step;

a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in said third step;

a seventh step of causing the intelligent interconnecting device to judge whether or not the

source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in said first step;

an eighth step of causing the intelligent interconnecting device to judge whether or not the source IP address is within a predetermined valid period when the source IP address of the external apparatus is judged to be identical with the stored source IP address in said seventh step;

a ninth step of determining the external apparatus having the source IP address which is judged to be within the predetermined valid period as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to execute the steps beginning from said second step, when the source IP address of the external apparatus is judged to be within the predetermined valid period in said eighth step; and

a tenth step of determining the external apparatus whose source IP address is judged to be non-identical or is judged to be not within the predetermined valid period as an apparatus not to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to store therein the source IP address of the external apparatus which is determined as the apparatus not to be responded to, when the source IP address of the external apparatus is judged to be non-identical with the stored source IP address in said seventh step or is judged to be not within the predetermined valid period in said eighth step.

8. An unauthorized access avoiding program which is executed in an intelligent interconnecting device having a function of repeating a packet which is transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol, preferably according to any one of claims 5 to 7, wherein the program comprises:

a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred;

a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in said first step that the first access from outside has occurred;

a third step of causing the intelligent interconnecting device to judge after the authentication processing in said second step whether or not authentication is given;

a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in said third step that the authentication is given;

a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from the external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in said fourth step;

a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in said third step;

a seventh step of causing the intelligent interconnecting device to judge whether or not the source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in said first step;

an eighth step of causing the intelligent interconnecting device to judge whether or not the source IP address is within a predetermined valid period when the source IP address of the external apparatus is judged to be identical with the stored source IP address in said seventh step;

a ninth step of determining the external apparatus having the source IP address which is judged to be within the predetermined valid period as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to execute the steps beginning from said second step, when the source IP address of the external apparatus is judged to be within the

predetermined valid period in said eighth step; and

a tenth step of determining the external apparatus whose source IP address is judged to be non-identical or is judged to be not within the predetermined valid period as an apparatus not to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to notify a predetermined managing computer of the source IP address of the external apparatus which is determined as the apparatus not to be responded to, when the source IP address of the external apparatus is judged to be non-identical with the stored source IP address in said seventh step or is judged to be not within the predetermined valid period in said eighth step.

9. Program according to claim 7, **characterized in that** the program further comprises an eleventh step of causing the intelligent interconnecting device to notify a predetermined managing computer of the source IP address of the external apparatus which is determined as the apparatus not to be responded to in said tenth step.

10. A recording medium in which a computer readable unauthorized access avoiding program executed in an intelligent interconnecting device having a function of repeating a packet which is transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol is recorded, wherein the program comprises:

a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred;

a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in the first step that the first access from outside has occurred;

a third step of causing the intelligent interconnecting device to judge after the authentication processing in the second step whether or not authentication is given;

a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in the third step that the authentication is given;

a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from the external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in the fourth step;

a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in the third step;

a seventh step of causing the intelligent interconnecting device to judge whether or not the source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in the first step;

an eighth step of determining the external apparatus whose source IP address is judged to be identical with the stored source IP address as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to process the steps beginning from the second step, when the source IP address of the external apparatus is judged to be identical with the stored source IP address in the seventh step; and

a ninth step of determining the external apparatus whose source IP address is judged to be non-identical with the stored source IP address as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the source IP address of the external apparatus is judged to be non-identical with the stored source IP address in the seventh step.

11. A recording medium in which a computer readable unauthorized access avoiding program executed in an intelligent interconnecting device having a function of repeating a packet transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol is recorded, preferably according to claim 10, wherein program comprises:

a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred;

a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in the first step that the first access from outside has occurred;

a third step of causing the intelligent interconnecting device to judge after the authentication processing in the second step whether or not authentication is given;

a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in the third step that the authentication is given;

a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from the external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in the fourth step;

a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in the third step;

a seventh step of causing the intelligent interconnecting device to judge whether or not the source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in the first step;

an eighth step of causing the intelligent interconnecting device to judge whether or not the source IP address is within a predetermined valid period when the source IP address of the external apparatus is judged to be identical with the stored source IP address in the seventh step;

a ninth step of determining the external apparatus having the source IP address which is judged to be within the predetermined valid period as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to execute the steps beginning from the second step, when the source IP address of the external apparatus is judged to be within the predetermined valid period in the eighth step; and

a tenth step of determining the external apparatus whose source IP address is judged to be non-identical or is judged to be not within the predetermined valid period as an apparatus not to be responded to thereafter by the intelligent interconnecting device, when the source IP address of the external apparatus is judged to be non-identical with the stored source IP address in the seventh step or is judged to be not within the predetermined valid period in the eighth step.

12. A recording medium in which a computer readable unauthorized access avoiding program executed in an intelligent interconnecting device having a function of repeating a packet transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol is recorded, preferably according to claim 10 or 11, wherein the program comprises:

a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred;

a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in the first step that the first access from outside has occurred;

a third step of causing the intelligent interconnecting device to judge after the authentication processing in the second step whether or not authentication is given;

a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in the third step that the authentication is given;

a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from the external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in the fourth step;

a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in the third step;

a seventh step of causing the intelligent interconnecting device to judge whether or not the source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in the first step;

an eighth step of causing the intelligent interconnecting device to judge whether or not the source IP address is within a predetermined valid period when the source IP address of the external apparatus is judged to be identical with the stored source IP address in the seventh step;

a ninth step of determining the external apparatus having the source IP address which is judged to be within the predetermined valid period as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to execute the steps beginning from the second step, when the source IP address of the external apparatus is judged to be within the predetermined valid period in the eighth step; and

a tenth step of determining the external apparatus whose source IP address is judged to be non-identical or is judged to be not within the predetermined valid period as an apparatus not to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to store therein the source IP address of the external apparatus which is determined as the apparatus not to be responded to, when the source IP address of the external apparatus is judged to be non-identical with the stored source IP address in the seventh step or is judged to be not within the predetermined valid period in the eighth step.

13. A recording medium in which a computer readable unauthorized access avoiding program executed in an intelligent interconnecting device having a function of repeating a packet transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol is recorded, preferably according to any one of claims 10 to 12, wherein the program comprises:

a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred;

a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in the first step that the first access from outside has occurred;

a third step of causing the intelligent interconnecting device to judge after the authentication processing in the second step whether or not authentication is given;

a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in the third step that the authentication is given;

a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from the external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in the fourth step;

a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in the third step;

a seventh step of causing the intelligent interconnecting device to judge whether or not the source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in the first step;

an eighth step of causing the intelligent interconnecting device to judge whether or not the source IP address is within a predetermined valid period when the source IP address of the external apparatus is judged to be identical with the stored source IP address in the seventh step;

a ninth step of determining the external apparatus having the source IP address which is judged to be within the predetermined valid period as an apparatus to be responded to there-

after by the intelligent interconnecting device and causing the intelligent interconnecting device to execute the steps beginning from the second step, when the source IP address of the external apparatus is judged to be within the predetermined valid period in the eighth step; and

a tenth step of determining the external apparatus whose source IP address is judged to be non-identical or is judged to be not within the predetermined valid period as an apparatus not to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to notify a predetermined managing computer of the source IP address of the external apparatus which is determined as the apparatus not to be responded to, when the source IP address of the external apparatus is judged to be non-identical with the stored source IP address in the seventh step or within the predetermined valid period in the eighth step.

14. Recording medium according to claim 12, **characterized in that** the program further comprises an eleventh step of causing the intelligent interconnecting device to notify a predetermined managing computer of the source IP address of the external apparatus which is determined as the apparatus not to be responded to by the intelligent interconnecting device in the tenth step.

15. Recording medium, preferably according to any one of claims 10 to 14, **characterized in that** a program according to any one of claims 5 to 9 is recorded on the recording medium.

16. An intelligent interconnecting device having a function of repeating a packet which is transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol, wherein the device comprises:

a LAN trunk line interfacing section having an interface function with a LAN trunk line;

a port interfacing section having an interface function with a terminal connected thereto;

a storage section for storing a program and data therein, and

a central controlling section for controlling operations of said LAN trunk line interfacing section, said port interfacing section, and said storage section, wherein said central controlling section executes the following steps:

to extract a source IP address included in a packet which is transmitted from an external apparatus and store it in said storage section when an access from the external apparatus is authenticated through execution of the TCP/IP protocol;

to judge, when an access from an external apparatus occurs thereafter, whether or not a source IP address of the external apparatus giving the access is identical with the stored source IP address; and

to permit communication thereafter with the external apparatus having the source IP address identical with the stored transmitting end IP address only when the source IP address is judged to be identical with the stored source IP address.

17. Device according to claim 16, **characterized in that**, when the source IP address is judged to be non-identical with the stored source IP address, said central controlling section registers the source IP address which is judged to be non-identical with the stored source IP address in an unauthorized access IP list.

18. Device according to claim 16 or 17, **characterized in that**, when the source IP address is judged to be non-identical with the stored source IP address, said controlling section notifies an authenticated managing computer of the source IP address which is judged to be non-identical with the stored source IP address.

19. Device according to any one of claims 16 to 18, **characterized in that**, when the source IP address is judged to be identical with the stored source IP address, said central controlling section judges whether or not the source IP address which is judged to be identical with the stored source IP address is within a valid period set in advance and permits communication thereafter between the external apparatus having the source IP address which is judged to be within the predetermined valid period and the intelligent interconnecting device only when it is judged to be within the valid period.

20. An intelligent interconnecting device having a function of repeating a packet which is transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol, preferably according to any one claims 16 to 19, wherein the device comprises:

a LAN trunk line interfacing section having an interface function with a LAN trunk line;

a port interfacing section having an interface function with a terminal connected thereto;

a storage section for storing a program and data therein; and

a central controlling section for controlling operations of said LAN trunk line interfacing section, said port interfacing section, and said storage section, wherein said central controlling section executes the following steps:

a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred;

a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in the first step that the first access from outside has occurred;

a third step of causing the intelligent interconnecting device to judge after the authentication processing in the second step whether or not authentication is given;

a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in the third step that the authentication is given;

a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from the external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in the fourth step;

a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in the third step;

a seventh step of causing the intelligent interconnecting device to judge whether or not the source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in the first step;

an eighth step of determining the external apparatus whose source IP address is judged to be identical with the stored source IP address as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to process the steps beginning from the second step when the source IP address of the external apparatus is judged to be identical with the stored source IP address in the seventh step; and

a ninth step of determining the external apparatus whose source IP address is judged to be non-identical with the stored source IP address as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the source IP address of the external apparatus is judged to be non-identical with the stored source IP address in the seventh step.

21. An intelligent interconnecting device having a function of repeating a packet which is transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol, preferably according to any one claims 16 to 20, wherein the device comprises:

a LAN trunk line interfacing section having an interface function with a LAN trunk line;

a port interfacing section having an interface function with a terminal connected thereto;

a storage section for storing a program and data therein; and

a central controlling section for controlling operations of said LAN trunk line interfacing section, said port interfacing section, and said storage section, wherein said central controlling section executes the following steps:

a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred;

a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in the first step that the first access from outside has occurred;

a third step of causing the intelligent interconnecting device to judge after the authentication processing in the second step whether or not authentication is given;

a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in the third step that the authentication is given;

a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from the external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in the fourth step;

a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in the third step;

a seventh step of causing the intelligent interconnecting device to judge whether or not the source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in the first step;

an eighth step of causing the intelligent interconnecting device to judge whether or not the source IP address is within a predetermined valid period when the source IP address of the external apparatus is judged to be identical with the stored source IP address in the seventh step;

a ninth step of determining the external apparatus having the source IP address which is judged to be within the predetermine valid period as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to execute the steps beginning from the second step, when the source IP address of the external apparatus is judged to be within the predetermined valid period in the eighth step; and

a tenth step of determining the external apparatus whose source IP address is judged to be non-identical or is judged to be not within the predetermined valid period as an apparatus not to be responded to thereafter by the intelligent interconnecting device, when the source IP address of the external apparatus is judged to be non-identical with the stored source IP address in the seventh step or is judged to be not within the predetermined valid period in the eighth step.

22. An intelligent interconnecting device having a function of repeating a packet which is transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol, preferably according to any one of claims 16 to 21, wherein the device comprises:

a LAN trunk line interfacing section having an interface function with a LAN trunk line;

a port interfacing section having an interface function with a terminal connected thereto;

a storage section for storing a program and data therein; and

a central controlling section for controlling operations of said LAN trunk line interfacing section, said port interfacing section, and said storage section, wherein said central controlling section executes the following steps:

a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred;

a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in the first step that the first access from outside has occurred;

a third step of causing the intelligent interconnecting device to judge after the au-

thentication processing in the second step whether or not authentication is given;

a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in the third step that the authentication is given;

a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from the external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in the fourth step;

a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in the third step;

a seventh step of causing the intelligent interconnecting device to judge whether or not the source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in the first step;

an eighth step of causing the intelligent interconnecting device to judge whether or not the source IP address is within a predetermined valid period when the source IP address of the external apparatus is judged to be identical with the stored source IP address in the seventh step;

a ninth step of determining the external apparatus having the source IP address which is judged to be within the predetermined valid period as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to execute the steps beginning from the second step, when the source IP address of the external apparatus is judged to be within the predetermined alid period in the eighth step; and

a tenth step of determining the external apparatus whose source IP address is judged to be non-identical or is judged to be not within the predetermined valid period as an apparatus not to be responded to thereafter by the intelligent interconnecting device and storing in said storage section the source IP address of the external apparatus which is determined as the apparatus not to be responded to, when the source IP address of the external apparatus is judged to be non-identical with the stored source IP address in the seventh step or is judged to be not within the predetermined valid period in the eighth step.

23. An intelligent interconnecting device having a function of repeating a packet which is transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol, preferably according to any one of claims 16 to 22, wherein the device comprises:

a LAN trunk line interfacing section having an interface function with a LAN trunk line;

a port interfacing section having an interface function with a terminal connected thereto;

a storage section for storing a program and data therein; and

a central controlling section for controlling operations of said LAN trunk line interfacing section, said port interfacing section, and said storage section, wherein said central controlling section executes the following steps:

a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred;

a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in the first step that the first access from outside has occurred;

a third step of causing the intelligent interconnecting device to judge after the authentication processing in the second step whether or not authentication is given;

a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing

the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in the third step that the authentication is given;

a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from the external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in the fourth step;

a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in the third step;

a seventh step of causing the intelligent interconnecting device to judge whether or not the source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in the first step;

an eighth step of causing the intelligent interconnecting device to judge whether or not the source IP address is within a predetermined valid period when the source IP address of the external apparatus is judged to be identical with the stored source IP address in the seventh step;

a ninth step of determining the external apparatus having the source IP address which is judged to be within the predetermined valid period as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to execute the steps beginning from the second step, when the source IP address of the external apparatus is judged to be within the predetermined valid period in the eighth step; and

a tenth step of determining the external apparatus whose source IP address is judged to be non-identical or is judged to be not within the predetermined valid period as an apparatus not to be responded to thereafter by the intelligent interconnecting device and notifying a predetermined managing computer of the source IP address of the external apparatus which is determined as the apparatus not to be responded to, when the source IP address of the external apparatus is judged to be non-identical with the stored source IP address in the seventh step or is judged to be not within the predetermined valid period in the eighth step.

24. Device according to claim 22, **characterized in that** said central controlling section executes an eleventh step of notifying a predetermined managing computer of the source IP address of the external apparatus which is determined as the apparatus not to be responded to in the tenth step.

25. A LAN system comprising an intelligent interconnecting device having a function of repeating a packet which is transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol, the intelligent interconnecting device being connected to a LAN trunk line while the plurality of computers being connected to the intelligent interconnecting device, wherein said intelligent interconnecting device is designed according to any one of claims 16 to 24.

FIG. 1

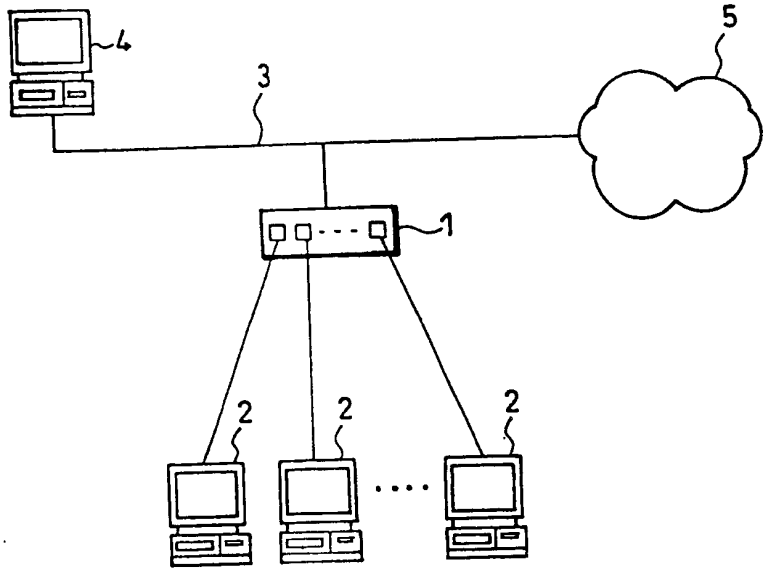

4
3
5
1
2
2
2

FIG. 2

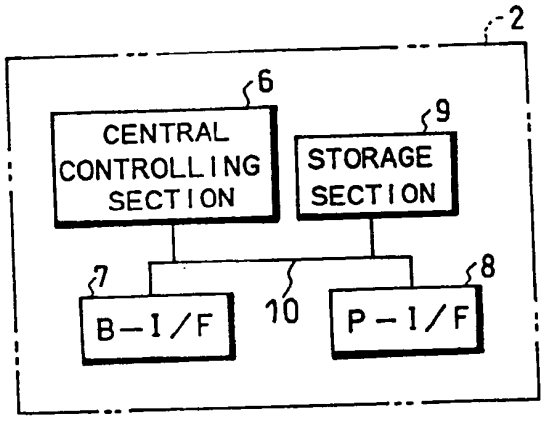

2
6
CENTRAL CONTROLLING SECTION
9
STORAGE SECTION
7
B-I/F
10
8
P-I/F

FIG. 3

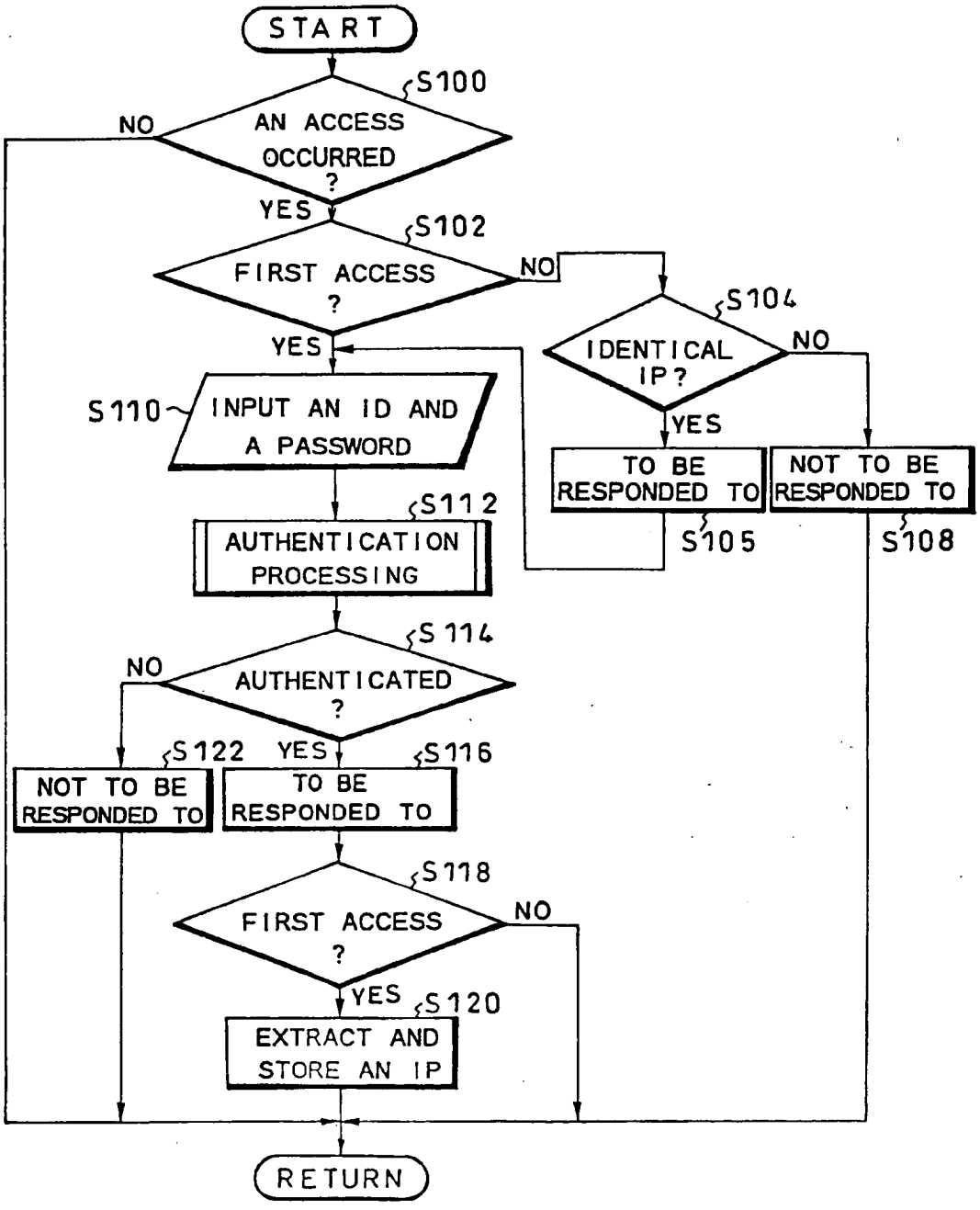
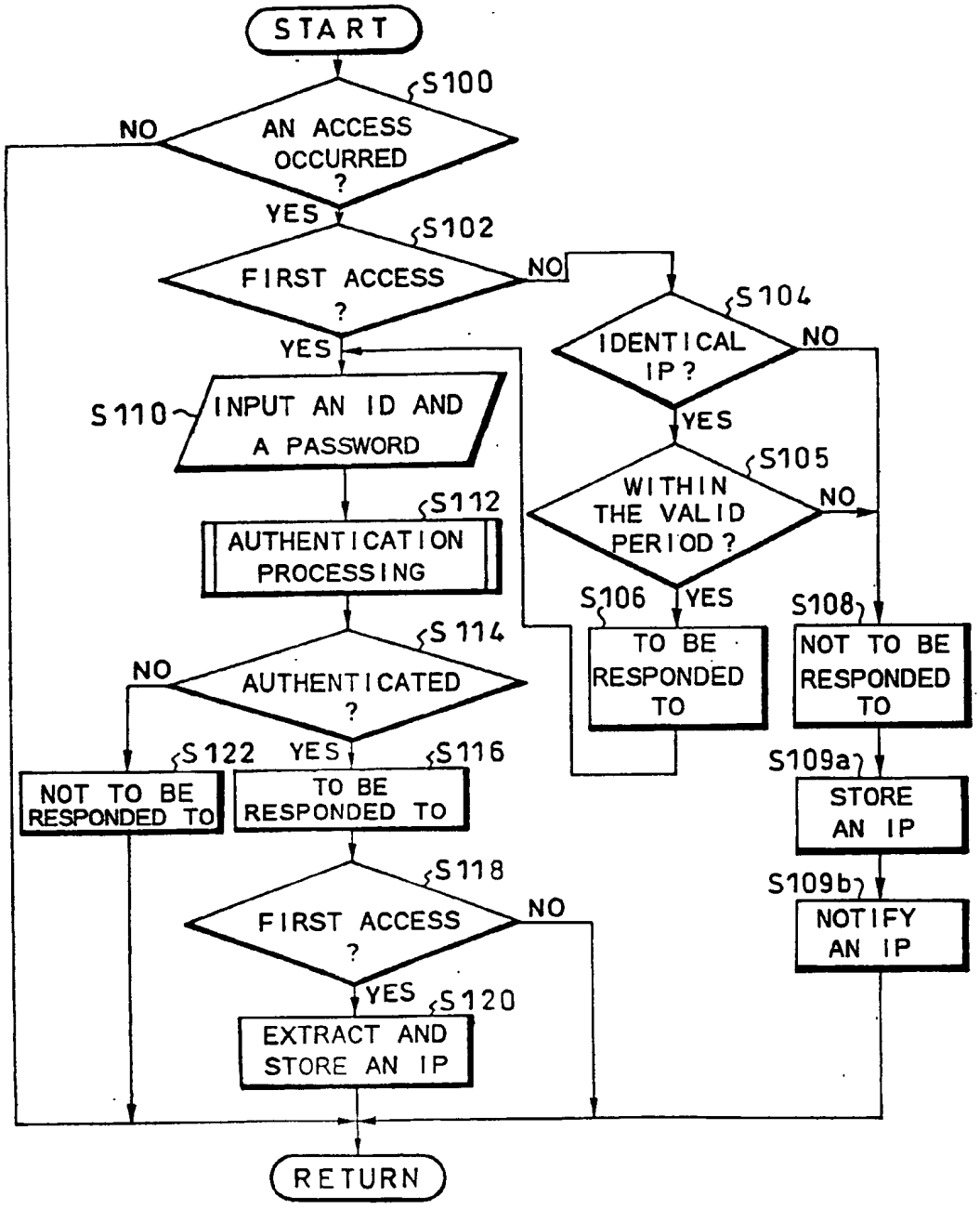

START
S100
AN ACCESS OCCURRED ?
NO
YES
S102
FIRST ACCESS ?
NO
YES
S104
IDENTICAL IP?
NO
YES
TO BE RESPONDED TO
S105
NOT TO BE RESPONDED TO
S108
S110
INPUT AN ID AND A PASSWORD
S112
AUTHENTICATION PROCESSING
S114
AUTHENTICATED ?
NO
YES
S122
NOT TO BE RESPONDED TO
S116
TO BE RESPONDED TO
S118
FIRST ACCESS ?
NO
YES
S120
EXTRACT AND STORE AN IP
RETURN

FIG. 4


START
S100
AN ACCESS OCCURRED ?
NO
YES
S102
FIRST ACCESS ?
NO
YES
S104
IDENTICAL IP ?
NO
YES
S105
WITHIN THE VALID PERIOD ?
NO
YES
S106
TO BE RESPONDED TO
S108
NOT TO BE RESPONDED TO
S109a
STORE AN IP
S109b
NOTIFY AN IP
S110
INPUT AN ID AND A PASSWORD
S112
AUTHENTICATION PROCESSING
S114
AUTHENTICATED ?
NO
YES
S116
TO BE RESPONDED TO
S118
FIRST ACCESS ?
NO
YES
S120
EXTRACT AND STORE AN IP
S122
NOT TO BE RESPONDED TO
RETURN

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 12 8220

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	US 6 202 156 B1 (KALAJAN KEVIN E) 13 March 2001 (2001-03-13) * abstract * * column 1, line 33 - column 2, line 23 * * column 2, line 66 - column 3, line 26 *	1,6,10, 16	H04L29/06
X	EP 0 909 072 A (LUCENT TECHNOLOGIES INC) 14 April 1999 (1999-04-14) * abstract * * page 2, line 33 - page 3, line 15 *	1,6,10, 16	
			TECHNICAL FIELDS SEARCHED (Int.Cl.7)
			H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	15 November 2002	Adkhis, F

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 01 12 8220

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

15-11-2002

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6202156 B1	13-03-2001	EP 1042744 A2	11-10-2000
		WO 9913448 A2	18-03-1999
EP 0909072 A	14-04-1999	US 6141749 A	31-10-2000
		EP 0909072 A2	14-04-1999
		JP 11163940 A	18-06-1999

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

State Intellectual Property Office of People's Republic of China

Add: 25/F., Bldg.B, Tsinghua Tongfang Hi-Tech Plaza, No.1, Wangzhuang Rd.,
Haidian District, Beijing , P. R. China, Postal Code:100083

Applicant(s)	SAMSUNG ELECTRONICS CO., LTD.	Issuing Date:
Patent Agent(s)	Zhimin RONG	September 15, 2006
Application No.	200410005804.7	
Title of Invention	Security Method for Operator Access Control of Network Management System	

THE FIRST OFFICE ACTION

1.☒ The applicant filed a request for substantive examination on _____(day/month/year). The examiner has carried out substantive examination on the above mentioned application for an invention patent in accordance with the provisions of Article 35(1) of the Chinese Patent Law.

☐ The Patent Office has decided to carry out substantive examination on the above mentioned application for an invention patent in accordance with the provisions of Article 35(2) of the Chinese Patent Law.

2. ☒ The applicant claimed:

the filing date 2003.2.19 in the Korea Patent Office as the priority date,
the filing date 2003.5.29 in the Korea Patent Office as the priority date,
the filing date _____ in the _____ Patent Office as the priority date,
the filing date _____ in the _____ Patent Office as the priority date,
the filing date _____ in the _____ Patent Office as the priority date.

☒ The applicant has provided a copy of the priority documents certified by the Patent Office where the prior application(s) was/were filed.

☐ The applicant has not provided a copy of the priority documents certified by the Patent Office where the prior application(s) was/were filed and the priority claim(s) is/are deemed not to have been made in accordance with the provisions of Article 30 of the Chinese Patent Law.

3.☐ The applicant submitted amendment (s) to the application on_____and on _____ , wherein, the amendment(s) submitted on _____ and
on _____ are unacceptable,
because said amendment(s) is/are not in conformity with

☐ the provisions of Article 33 of the Chinese Patent Law:

☐ the provisions of Rule 51 of the Implementing Regulations of the Chinese Patent Law.

The detailed reasons for the amendments being unacceptable are described in the text of this Office Action.

4. ☒The examination was carried out based on the application documents originally filed.

☐The examination was carried out based on the application documents indicated below:

☐Description:

Pages _____ of original application documents filed on the application date,
Pages _____ filed on; Pages_____ filed on;

Pages _____ filed on; Pages_____ filed on;

☐Claims:
Pages _____ of original application documents filed on the application date,
Pages _____ filed on; Pages_____ filed on;
Pages _____ filed on; Pages_____ filed on;

☐Drawings:
Pages _____ of original application documents filed on the application date,
Pages _____ filed on; Pages_____ filed on;
Pages _____ filed on; Pages_____ filed on;

☐Abstract: ☐ Filed on the application date; ☐ filed on _____

☐Drawing selected for publication on the front page of the application: ☐ Filed on the application date; ☐ filed on _____

5.☐ This Notification is issued without a search having been conducted.
☒ This Notification is issued with a search having been conducted.
☒ The following reference documents have been cited in this office action (their serial numbers will be referred to in the ensuing examination procedure):

Serial No.	Reference document(Number or Title)	Publication Date (or Filing date of interference patent applications)
1	**EP1274212A1**	**08**day **01** month **2003** year
2		day month year
3		day month year
4		day month year

6. The result of the examination is as follows:
☒ Description:
☐ The subject matter of the application falls into the scope on which no patent rights shall be granted as provided by Article 5 of the Chinese Patent Law.
☐ The description is not in conformity with the provisions of Article 26(3) of the Chinese Patent Law.
☒ The description is not in conformity with the provisions of Rule 18 of the Implementing Regulations of the Chinese Patent Law.

☒ Claims:
☒ Claims 7-12 falls into the scope, on which no granted patent rights shall be granted, as provided by Article 25 of the Chinese Patent Law.
☐ Claim _____ is not in conformity with the definition of invention as prescribed by Rule 2(1) of the Implementing Regulations of the Chinese Patent Law.
☐ Claim _____ does not possess novelty as provided by Article 22(2) of the Chinese Patent Law.

☒ Claims 1, 6 does not possess inventiveness as provided by Article 22(3) of the Chinese Patent Law.

☐ Claim _____ does not possess practical applicability as provided by Article 22(4) of the Chinese Patent Law.

☒ Claim 2 is not in conformity with the provisions of Article 26(4) of the Chinese Patent Law.

☐ Claim _____ is not in conformity with the provisions of Article 31(1) of the Chinese Patent Law.

☒ Claims 3, 4 is not in conformity with the provisions of Rule 20 of the Implementing Regulations of the Chinese Patent Law.

☐ Claim _____is not in conformity with the provisions of Article 9 of the Chinese Patent Law.

☐ Claim _____is not in conformity with the provisions of Rule 12(1) of the Implementing Regulations of the Chinese Patent Law.

The detailed reasoning for the above opinion is described in the text of this office action.

7. On the basis of the above opinion, the examiner holds that:

☐ The applicant should make amendments as required in the text of this office action.

☒ The applicant should provide reasons for that the above mentioned patent application can be granted patent right, and make amendments to the specification as described in the text of this office action; otherwise the patent right shall not be granted.

☐ The patent application does not possess any substantive contents for which patent right may be granted, if the applicant fails to provide reasons or the reasons provided are not sufficient, this application will be rejected.

8. The applicant's attention is drawn to the following matters:

(1) In accordance with the provisions of Article 37 of the Chinese Patent Law, the applicant shall submit a response within four months from the date of receiving this office action. If the applicant fails to meet the time limit without any justified reason, the application shall be deemed to have been withdrawn.

(2) The amendment made by the applicant shall be in conformity with the provisions of Article 33 of the Chinese Patent Law. The amendment shall be submitted in duplicate copies and in the format required by the relevant provisions of the Examination Guideline.

(3) The applicant's response and/or amended documents shall be mailed or submitted to the Receiving Department of the Chinese Patent Office. Documents which are not mailed or submitted to the Receiving Department do not possess legal effect.

(4) The applicant and/or his(its) agent shall not come to the Chinese Patent Office for interview with the examiner without an appointment.

9. The text of this office action consists of a total of 2 sheets, and is accompanied by the following annexes:

☒ A copy of the cited reference documents consisting of 1 set and 22 sheets.

☐

The _____ Examination Department

The Seal of the Examiner: Rui PENG

中华人民共和国国家知识产权局

邮政编码：100083 北京市海淀区王庄路1号清华同方科技大厦B座25层 中科专利商标代理有限责任公司 戎志敏	发文日期
申请号：2004100058047	
申请人：三星电子株式会社	
发明创造名称：网络管理系统的操作员存取控制的安全方法	

第一次审查意见通知书

1. ☑应申请人提出的实审请求，根据专利法第35条第1款的规定，国家知识产权局对上述发明专利申请进行实质审查。
   ☐根据专利法第35条第2款的规定，国家知识产权局决定自行对上述发明专利申请进行审查。
2. ☑申请人要求以其在：
   KR 专利局的申请日 2003年02月19日为优先权日，
   KR 专利局的申请日 2003年05月29日为优先权日，
   专利局的申请日 年 月 日为优先权日，
   专利局的申请日 年 月 日为优先权日，
   专利局的申请日 年 月 日为优先权日。
   ☑申请人已经提交了经原申请国受理机关证明的第一次提出的在先申请文件的副本。
   ☐申请人尚未提交经原申请国受理机关证明的第一次提出的在先申请文件的副本，根据专利法第30条的规定视为未提出优先权要求。
3. ☐经审查，申请人于：
   年 月 日提交的 不符合实施细则第51条的规定；
   年 月 日提交的 不符合专利法第33条的规定：
   年 月 日提交的
4. 审查针对的申请文件：
   ☑原始申请文件。 ☐审查是针对下述申请文件的
   申请日提交的原始申请文件的权利要求第 项、说明书第 页、附图第 页；
   年 月 日提交的权利要求第 项、说明书第 页、附图第 页；
   年 月 日提交的权利要求第 项、说明书第 页、附图第 页；
   年 月 日提交的权利要求第 项、说明书第 页、附图第 页；
   年 月 日提交的说明书摘要， 年 月 日提交的摘要附图。
5. ☐本通知书是在未进行检索的情况下作出的。
   ☑本通知书是在进行了检索的情况下作出的。
   ☑本通知书引用下述对比文献（其编号在今后的审查过程中继续沿用）：

编号	文件号或名称	公开日期（或抵触申请的申请日）
1	EP1274212A1	2003-01-08

6. 审查的结论性意见：
   ☐关于说明书：
   ☐申请的内容属于专利法第5条规定的不授予专利权的范围。
   ☐说明书不符合专利法第26条第3款的规定。

☐说明书不符合专利法第 33 条的规定。
☑说明书的撰写不符合实施细则第 18 条的规定。
☐_____

☑关于权利要求书：
☐权利要求_____不具备专利法第 22 条第 2 款规定的新颖性。
☑权利要求 1,6 不具备专利法第 22 条第 3 款规定的创造性。
☐权利要求_____不具备专利法第 22 条第 4 款规定的实用性。
☑权利要求 7-12 属于专利法第 25 条规定的不授予专利权的范围。
☑权利要求 2 不符合专利法第 26 条第 4 款的规定。
☐权利要求_____不符合专利法第 31 条第 1 款的规定。
☐权利要求_____不符合专利法第 33 条的规定。
☐权利要求_____不符合专利法实施细则第 2 条第 1 款关于发明的定义。
☐权利要求_____不符合专利法实施细则第 13 条第 1 款的规定。
☑权利要求 3、4 不符合专利法实施细则第 20 条的规定。
☐权利要求_____不符合专利法实施细则第 21 条的规定。
☐权利要求_____不符合专利法实施细则第 22 条的规定。
☐权利要求_____不符合专利法实施细则第 23 条的规定。
☐_____

上述结论性意见的具体分析见本通知书的正文部分。

7. 基于上述结论性意见，审查员认为：
☐申请人应按照通知书正文部分提出的要求，对申请文件进行修改。
☑申请人应在意见陈述书中论述其专利申请可以被授予专利权的理由，并对通知书正文部分中指出的不符合规定之处进行修改，否则将不能授予专利权。
☐专利申请中没有可以被授予专利权的实质性内容，如果申请人没有陈述理由或者陈述理由不充分，其申请将被驳回。
☐_____

8. 申请人应注意下述事项：
(1) 根据专利法第 37 条的规定，申请人应在收到本通知书之日起的肆个月内陈述意见，如果申请人无正当理由逾期不答复，其申请将被视为撤回。
(2) 申请人对其申请的修改应符合专利法第 33 条的规定，修改文本应一式两份，其格式应符合审查指南的有关规定。
(3) 申请人的意见陈述书和/或修改文本应邮寄或递交国家知识产权局专利局受理处，凡未邮寄或递交给受理处的文件不具备法律效力。
(4) 未经预约，申请人和/或代理人不得前来国家知识产权局专利局与审查员举行会晤。

9. 本通知书正文部分共有 2 页，并附有下述附件：
☑引用的对比文件的复印件共 1 份 22 页。☐_____

审查员：彭锐(3124)
2006 年 8 月 22 日

彭锐 印

审查部门 通信审查部

回函请寄：100088 北京市海淀区蓟门桥西土城路 6 号 国家知识产权局专利局受理处收
（注：凡寄给审查员个人的信函不具有法律效力）